Integration Middleware Forms Vital Link in IoT Ecosystems

Abstract

The Internet of Things (IoT) is a rapidly growing and evolving domain. High interconnectivity and huge data volumes make setting up an IoT ecosystem a complex and challenging task. To ensure effective data management, it is vital to focus on design, implementation, integration, and security.

With the emergence of embedded systems, the line between software and hardware has blurred. Middleware is the vital fabric that stitches together the various elements and components of an application ecosystem. It provides a clear standards-based framework for data exchange within and outside an enterprise.
The IoT Holds the Key to the Future

Organizations across industries can benefit immensely from the rich, context-sensitive data provided by IoT ecosystems. Using advanced analytics tools, this data can help organizations make accurate business decisions in a timely manner. Being data-driven, IoT ecosystems allow enterprises to respond and react to evolving market requirements and plan operations better, based on the information gathered from connected devices. In some cases, the insights open up new growth areas and reveal untapped potential within the enterprise.

The adoption and integration of the right middleware product is vital to successful IoT implementations. However, IoT middleware is considerably complex by architecture, and challenging to implement.

The IoT architecture is composed of five layers:

- The physical layer gathers data from the environment and passes it on for collation, analysis, and decision-making.
- The communication layer establishes communication channels between numerous IoT devices operating at the physical and software layers.
- The integration and middleware layer integrates IoT devices and enterprise applications.

A 2015 IDC report expects the worldwide spending on IoT to grow at a 17.0% compound annual growth rate (CAGR) from $698.6 billion in 2015 to nearly $1.3 trillion in 2019¹.

To maximize the IoT advantage, it is essential to understand how and where different components of the IoT are leveraged in order to deliver connected services to end users.
The storage layer leverages Big Data and NoSQL technologies to store the vast amount of IoT data flowing into an enterprise.

The processing and presentation layer processes IoT data and presents it to the respective applications for analysis and consumption by business users.

Data flow in an IoT ecosystem

An IoT ecosystem continuously generates huge amounts of complex data, which need to be integrated, stored, and processed by an enterprise to realize its potential benefits. At a high level, the primary components of an IoT ecosystem are:

- **Enterprise applications**: Numerous devices and sensors can be enabled and integrated on the IoT grid to collect and pass data back to enterprise business analytics engines.

- **IoT data store**: Depending on the nature (structured or unstructured), volume, variety, and throughput, the data store for an IoT ecosystem can be determined.

- **IoT infrastructure**: To successfully define, integrate, and implement all these components, a strong, scalable underlying infrastructural framework is needed with just-in-time infrastructure provisioning and cloud computing capabilities.

Of all IoT ecosystem components—devices and sensors, routers, gateways, middleware, and mobile devices and applications—middleware is the most important. As the IoT connects multiple devices, it provides nodes for device, application, and data integration at various levels. The
middleware provides a fast, secure, and reliable channel for the transport and exchange of data within an enterprise and beyond. However, this requires additional characteristics such as device abstraction, interface protocols, multi-context management, and application abstraction—within a robust security and management framework.

Conventional versus IoT Middleware

Conventional middleware systems form the bridge between various applications, helping them communicate and exchange information. Its functional blocks include:

- **Integration**: The integration layer communicates and interfaces with other layers or systems using built-in protocols of the middleware suite, and is responsible for providing a safe and secure channel of communication.

- **Conversion**: Middleware serves as a mechanism to transport data from one application to another. Sometimes the data format between applications is incompatible. Middleware can perform this function much more efficiently and successfully than the application layer.

- **Routing**: There are different ways to accomplish routing, including JMS, SOAP, REST, and WS, among others. Some integration middleware vendors like TIBCO have their own proprietary routing mechanism to enable faster delivery.

In case of the IoT, along with these standard functional blocks, we also need:

- Compliance with multiple industry standards
- Multi-layered physical and logical security at each integration touch-point
- Scalability to accommodate future business requirements
- High data throughput to handle huge volumes flowing from sensors and devices
- Support for multiple protocols and interoperability frameworks to import and export information seamlessly
- Multi-device integration capability

The interplay of these factors makes the adoption of IoT middleware considerably challenging compared to conventional middleware implementation.
Key Challenges in IoT Middleware Implementation

Choosing a middleware product and implementing it in the enterprise framework for an IoT solution poses some challenges:

- **Service orientation:** Organizations are gradually moving to the service oriented architecture (SOA) model. To meet evolving business requirements, new features are introduced by combining services in a cross-layer form.

- **Application integration:** The IoT needs two-way, real-time communication between software applications and devices. Providing APIs for remote access to historical device data is not enough to accomplish this. Most IoT use cases will not work without application integration.

- **Data integration:** IoT devices send data in different formats, using different interfaces. In many instances, they communicate with the outside world and share relevant data. Data integration is therefore a critical success factor for an IoT initiative.

Proposed Approaches to Deploying IoT Middleware

**Traditional data center deployment approach**

The future of the IoT is expected to involve a more open architecture model, which pushes the application layer closer to the external connectivity layer. This will free up the enterprise network from the continuous task of large data transfers. However the large amounts of data generated by IoT ecosystems will need to be stored, processed, and analyzed in near-real time, which will increase the data center workload. Hence, the traditional data center will need to be redesigned to accommodate timely ramp-up of vital resources such as servers, storage, and network.

**Cloud deployment approach**

For the IoT to achieve the desired scalability and ramp-up, the traditional data center approach may not be ideal as it involves high capital and operational expenditure. Further, this infrastructure may be unable to keep pace with rapid technological advances and evolving business requirements.

Some specialized IoT solutions with scalable middleware framework available today are:

- IBM Watson IoT Solutions
- Oracle Fusion Middleware
- Microsoft Azure IoT
- LinkSmart
- AWS IoT solutions
- UBISOAP
A viable alternative involves a public cloud (Internet-based) or a private cloud (intranet-based) offering that shares configurable processing resources and data with computers and other devices on demand—networks, servers, storage, applications, and services, which can be rapidly commissioned and de-commissioned with minimal management effort. This results in huge capex and opex savings for enterprises.

The benefits of a cloud-based approach include the ability to scale rapidly, a common platform for all IoT ecosystem components, high availability and fault tolerance, and lower cost of operations.

Conclusion

With IoT ecosystems gaining widespread adoption across industries, companies will need to devise appropriate implementation strategies to achieve the desired business outcomes. IoT middleware is probably the most critical link in the entire setup.

The management of IoT middleware has subtle differences with traditional middleware administration. The scale of operations, multiple interfaces requirements, standards compliance, and the multi-vendor ecosystem make it considerably complex. Therefore, IoT middleware deployment, monitoring, administration, and management need to be underpinned with the basic philosophy of interoperable services—available anytime, anywhere, and on any device.

Clearly, there is no one-size-fits-all approach when it comes to IoT middleware. The right focus and investment will prove to be the differentiating factor for enterprises, as they adopt this fast-growing, business-critical technology.

References

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com